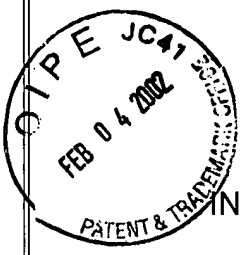
#2



Customer Number 22,852
Attorney Docket No. 05905.0154

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventors: Takao MIYOSHI et al.	)	
Serial No.: 10/021,027	)	Group Art Unit: 2673
Filed: December 19, 2001	)	
For: SECURITY SYSTEM	)	

Assistant Commissioner for Patents
Washington, DC 20231

Sir:

CLAIM FOR PRIORITY

Under the provisions of Section 119 of 35 U.S.C., applicants hereby claim the benefit of the filing date of Japanese Patent Application No. 2000-387833, filed on December 20, 2000, for the above-identified United States Patent Application.

In support of applicants' claim for priority, filed herewith is one certified copy of the above.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: 2/4/02

By: _____
Richard V. Burgujian
Reg. No. 31,744

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年１２月２０日

出願番号
Application Number: 特願２０００－３８７８３３

[ST.10/C]: [ＪＰ２０００－３８７８３３]

出願人
Applicant(s): 株式会社セガ

２００２年　１月１１日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３１１５０１７

【書類名】　特許願

【整理番号】　S007P3P111

【あて先】　特許庁長官殿

【発明者】

【住所又は居所】　東京都大田区羽田１丁目２番１２号
株式会社ソニックチーム内

【氏名】　見吉　隆夫

【発明者】

【住所又は居所】　東京都大田区羽田１丁目２番１２号
株式会社ソニックチーム内

【氏名】　節政　暁生

【特許出願人】

【識別番号】　000132471

【氏名又は名称】　株式会社セガ

【代理人】

【識別番号】　100079108

【弁理士】

【氏名又は名称】　稲葉　良幸

【選任した代理人】

【識別番号】　100080953

【弁理士】

【氏名又は名称】　田中　克郎

【選任した代理人】

【識別番号】　100093861

【弁理士】

【氏名又は名称】　大賀　眞司

【手数料の表示】

【予納台帳番号】　011903

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9706518

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　セキュリティシステム

【特許請求の範囲】

【請求項１】　通信ネットワークに接続するデータ処理装置に固有の識別情報を発行する手段と、該データ処理装置に固有の識別情報と該データ処理装置にて処理されるべきデータを記録した記録媒体に固有の識別情報とを関連付けて記憶する手段と、該関連付けを参照することで何れの記録媒体が何れのデータ処理装置で使用されたかを管理する手段と、を備えたセキュリティシステム。

【請求項２】　前記データ処理装置に固有の識別情報として、データ処理装置が通信ネットワークに接続した時期又はこれを利用した情報を用いる請求項１に記載のセキュリティシステム。

【請求項３】　通信ネットワークに接続するデータ処理装置に固有の識別情報を発行し、該データ処理装置に固有の識別情報と該データ処理装置にて処理されるべきデータを記録した記録媒体に固有の識別情報とを関連付けて記憶し、該関連付けを参照することで何れの記録媒体が何れのデータ処理装置で使用されたかを管理する記録媒体管理方法。

【請求項４】　前記データ処理装置に固有の識別情報として、データ処理装置が通信ネットワークに接続した時期又はこれを利用したを用いる請求項３に記載の記録媒体管理方法。

【請求項５】　請求項３又は請求項４に記載の記録媒体管理方法をコンピュータシステムに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項６】　通信ネットワークを介してサーバから発行されるデータ処理装置に固有の第１識別情報を記憶する記憶手段と、データを記録した記録媒体に固有の識別情報であって上記第１識別情報とともに関連付けられて記録媒体の管理に用いられる第２識別情報を第１識別情報とともに通信ネットワークを介してサーバに送信する送信手段と、を備えたデータ処理装置。

【請求項７】　コンピュータシステムを請求項６に記載の記憶手段、及び送信手段として機能させるプログラムを記録したコンピュータ読み取り可能な記録

媒体。

【請求項８】　バックアップメモリのセーブデータをデータ処理するデータ処理装置であって、セーブデータを該データ処理装置に固有の識別情報をキーとして暗号化処理する手段を備えたデータ処理装置。

【請求項９】　前記暗号化処理されたセーブデータを前記識別情報をキーとして復号化処理する手段を備えた請求項８に記載のデータ処理装置。

【請求項１０】　バックアップメモリのセーブデータをデータ処理装置に固有の識別情報をキーとして暗号化処理するデータ処理方法。

【請求項１１】　前記暗号化処理されたセーブデータを前記識別情報をキーとして復号化処理する請求項１０に記載のデータ処理方法。

【請求項１２】　請求項１０又は請求項１１に記載のデータ処理方法をデータ処理装置に実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１３】　バックアップメモリに記憶されているセーブデータを読み取って記憶する手段と、該セーブデータの読み取り終了後にバックアップメモリに記憶されているセーブデータを消去する手段と、を備えたデータ処理装置。

【請求項１４】　データ処理装置にてデータ処理されるセーブデータをデータ処理装置に転送した後で、バックアップメモリ内の不揮発性メモリに記憶されたセーブデータを消去するセーブデータの管理方法。

【請求項１５】　バックアップメモリを備えたデータ処理装置が通信ネットワークに接続した回数をデータベースに登録するとともに、上記回数をバックアップメモリ又はデータ処理装置に記録する手段と、バックアップメモリを備えたデータ処理装置が通信ネットワークに接続した際にデータ処理装置から取得した上記回数がデータベースに登録されている回数と一致した場合にバックアップメモリ内のデータの処理を許可する手段とを備えたセキュリティシステム。

【請求項１６】　前記バックアップメモリに固有の識別情報として、バックアップメモリを備えたデータ処理装置が通信ネットワークに接続した時期又はこれを利用した情報を用いる請求項１５に記載のセキュリティシステム。

【請求項１７】　バックアップメモリを備えたデータ処理装置が通信ネット

ワークに接続した回数をデータベースに登録するとともに、上記回数をバックアップメモリ又はデータ処理装置に記録し、バックアップメモリを備えたデータ処理装置が通信ネットワークに接続した際にデータ処理装置から取得した上記回数がデータベースに登録されている回数と一致した場合にバックアップメモリ内のデータの処理を許可するセーブデータの管理方法。

【請求項１８】　前記バックアップメモリに固有の識別情報として、バックアップメモリを備えたデータ処理装置が通信ネットワークに接続した時期又はこれを利用した情報を用いる請求項１７に記載のバックアップメモリ管理方法。

【請求項１９】　請求項１７又は請求項１８に記載のバックアップメモリ管理方法をコンピュータシステムに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項２０】　ゲームの難易度に対応して通信ゲームに参加可能なレベルを予め設定し、ゲームの難易度に対応した要求レベルを満たすプレイヤに対して通信ゲームの参加を許可するゲームサーバ。

【請求項２１】　通信ネットワークに接続して通信ゲームを行うときにはゲームの進行状況をセーブデータとして保存しないゲーム処理方法。

【請求項２２】　請求項２１に記載のゲーム処理方法をゲーム装置に実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項２３】　通信ネットワークに接続して通信ゲームを行うときにはゲームのエンディング画面の表示時間を短くするゲーム処理方法。

【請求項２４】　請求項２３に記載のゲーム処理方法をゲーム装置に実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は複数のゲーム装置がネットワークに接続して行う通信ゲームの改良技術に関する。

【０００２】

【従来の技術】

複数のゲーム装置が電話回線、ＩＳＤＮ網等の通信ットワークに接続し、通信ゲームを行うことが提案されている。かかる通信ゲームにおいて、本出願人はゲームソフトウエアを記録した記録媒体の第三者による不正使用を防止するべく、特開平２０００－３５８８５号にて記録媒体のセキュリティ技術を提案した。

【０００３】

同公報に記載の技術はゲームソフトウエアを記録した記録媒体に固有の識別情報とゲーム装置に固有の識別情報をサーバが一元管理し、どのゲーム装置がどの記録媒体を使用したかを把握しておくことで、ゲーム装置が通信ットワークに接続したときに、そのゲーム装置に装着された記録媒体が以前に他のゲーム装置に使用されたものであるとサーバが判断したときにはゲーム処理に制限を設け、当該ゲーム装置にのみ使用されたものであるとサーバが判断したときには通常のゲーム処理を行うというものである。

【０００４】

【発明が解決しようとする課題】

しかし、ゲーム装置に固有の識別情報は必ずしもゲーム装置の開発の段階で予め入れておくとは限らないため、このような識別情報を持たないゲーム装置も存在する。

【０００５】

また、通信ゲームにおいては、ゲーム装置本体或いは操作用コントローラに脱着可能に構成されたバックアップメモリにゲームの進行状況やプレイヤが獲得した各種アイテム等のデータを待避保存しておくことで、ゲーム終了直前の状態から再びゲームプレイを行うことができていたが、バックアップメモリの内容をコピーすることで、第三者に自己のセーブデータ（例えば、アイテム等）を提供することができるため、当該第三者は他人のセーブデータを利用してゲームを楽しむことができた。このようにバックアップメモリの内容が容易にコピーされると、プレイヤがゲームの面白さを味わうことができないという不具合が生じる。

【０００６】

このような問題はゲーム装置本体或いは操作用コントローラに脱着可能に構成されたバックアップメモリを他人のゲーム装置本体或いは操作用コントローラに

装着してゲームプレイを行うことができるように構成した場合にも生じる。

【０００７】

また、バックアップメモリに待避保存されたセーブデータを通信ネットワークを介してゲーム装置から他のゲーム装置に転送することができるが、バックアップメモリからゲーム装置にセーブデータを転送する際にバックアップメモリ内にセーブデータを残しておくと、バックアップメモリをゲーム装置から強制的に抜き取ることで自己のバックアップメモリにセーブデータを残したまま、他人にセーブデータを提供することができるという不正使用がなされるおそれがある。

【０００８】

また、従来の通信ゲームにおいてはゲームに参加可能なレベルに制限を設けなかったため、例えば、初心者と上級者が通信ゲームに参加する場合には、初心者は何もしなくても上級者の後をつけて行くことでゲームのエンディングにまで辿り着いてしまうことになり、ゲームの面白さが半減する結果となっていた。

【０００９】

同様に、複数の遊戯者が参加する通信ゲームの場合にゲームの進行状況に関するセーブデータを待避保存しておくと、初心者は上級者とともにゲームに参加することで上級者のゲームの途中からゲームを進めることとなってしまう。初心者のバックアップメモリにゲームの進行状況に関するセーブデータを保存してしまうと、次回のゲームはこの途中から開始することとなってしまい、ゲームの一部がプレイできなくなってしまうままになるため望ましくない。

【００１０】

また、通信ゲームの場合は電話回線に接続している限り、接続料として電話料金が課金され、さらにプロバイダへのインターネット接続料も課金されるため、遊戯者の操作を必要としないゲームのエンディングが必要以上に長時間を要すると、プレイヤはゲームプレイをしていないのにもかかわらず、過大な経済的負担を強いられる結果となる。

【００１１】

そこで本発明は、第三者による記録媒体の不正使用を防止するセキュリティシステム、データ処理装置、記録媒体管理方法及び該方法を実行するためのプログ

ラムを記録したコンピュータ読み取り可能な記録媒体を提案することを課題とする。また本発明はバックアップメモリの不正使用を防止するデータ処理装置、データ処理方法、セキュリティシステム、セーブデータの管理方法及び該方法を実行するためのプログラムを記録したコンピュータ読み取り可能な記録媒体を提案することを課題とする。また本発明は通信ゲームをより面白く楽しむためのゲームサーバ、ゲーム処理方法及び該方法を実行するためのプログラムを記録したコンピュータ読み取り可能な記録媒体を提案することを課題とする。

【００１２】

【課題を解決するための手段】

上記の課題を解決するべく、本発明では通信ネットワークに接続するデータ処理装置に固有の識別情報を発行し、該データ処理装置に固有の識別情報と該データ処理装置にて処理されるべきデータを記録した記録媒体に固有の識別情報とを関連付けて記憶し、該関連付けを参照することで何れの記録媒体が何れのデータ処理装置で使用されたかを管理する。データ処理装置の識別情報は通信ネットワークを介してサーバが発行するため、予め固有の識別情報を持たないデータ処理装置であっても、記録媒体のセキュリティを確保することができる。

【００１３】

また本発明では上記の方法をコンピュータシステムに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することができる。コンピュータ読み取り可能な記録媒体として、例えば、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＤＶＤ－Ｒ、ＰＤディスク、ＭＤディスク、ＭＯディスク等の固有の物理フォーマットをもつディスク）やフレキシブルディスク（ＦＤ）のように可搬性記録媒体の他、ＲＡＭやＲＯＭ等のコンピュータ内の内部記憶装置、或いはハードディスクのような外部記憶装置等がある。

【００１４】

また本発明ではバックアップメモリのセーブデータをデータ処理装置に固有の識別情報をキーとして暗号化処理する。これにより、バックアップメモリ内のセーブデータは他のデータ処理装置では使用できないため、セーブデータの不正使用を防止することができる。

【００１５】

また本発明ではデータ処理装置にてデータ処理されるセーブデータをデータ処理装置に転送した後で、バックアップメモリ内の不揮発性メモリに記憶されたセーブデータを消去する。これにより、バックアップメモリ内のセーブデータを該バックアップメモリ内に残したまま他のデータ処理装置に転送するという不正使用を有効に防止することができる。

【００１６】

また本発明ではバックアップメモリを備えたデータ処理装置が通信ネットワークに接続した回数をデータベースに登録するとともに、上記回数をバックアップメモリ又はデータ処理装置に記録し、バックアップメモリを備えたデータ処理装置が通信ネットワークに接続した際にデータ処理装置から取得した上記回数がデータベースに登録されている回数と一致した場合にバックアップメモリ内のデータの処理を許可する。これにより、バックアップメモリ内のセーブデータの不正コピーを有効に防止することができる。

【００１７】

また本発明ではゲームの難易度に対応して通信ゲームに参加可能なレベルを予め設定し、ゲームの難易度に対応した要求レベルを満たすプレイヤに対して通信ゲームの参加を許可する。これにより、初級者が上級者とともに通信ゲームに参加することで上級者の力を借りてゲームを進行するという上記の不都合を解消することができる。

【００１８】

また本発明では通信ネットワークに接続して通信ゲームを行うときにはゲームの進行状況をセーブデータとして保存しない。また、ゲーム装置がゲーム進行の状況を保存する場合であっても、通信ネットワークに接続しないでゲームを行うときには該進行状況を参照してゲームの途中からプレイすることを禁じるように構成してもよい。これにより、上記の不都合を解消することができる。

【００１９】

また本発明では通信ネットワークに接続して通信ゲームを行うときにはゲームのエンディング画面の表示時間を短くする。これにより通信ネットワークの接続

料やゲームサーバへのインターネット接続料の増額を抑えることができる。

【００２０】

【発明の実施の形態】

発明の実施の形態１．

図１は記録媒体の第三者による不正使用を防止するサーバとゲーム装置の説明図である。同図において、符号１０はＣＤ－ＲＯＭ等のゲームソフトウエアを記録した可搬性記録媒体であり、符号１１は家庭用ゲーム装置である。ゲーム装置１１は記録媒体１０に記録されているゲームプログラムを読み取り、電話回線、ＩＳＤＮ網等の各種公衆回線或いは専用線等の通信ネットワークを介して他のゲーム装置と共に通信ゲームを行うことができるように所望の通信機能を備えて構成されている。サーバ１３は通信ットワークに接続する各々のゲーム装置の通信ゲーム処理等を管理する。

【００２１】

記録媒体１０にはシリアルナンバー（ＳＮ）と呼ばれる各記録媒体に固有の識別情報が与えられている。同図の例では記録媒体のＳＮはＡ０１０１である。ＳＮは記録媒体１０にデータとして記録されているものでもよく、記録媒体１０或いはその収納ケースやマニュアルに記載されているものでもよい。ゲーム装置１１が通信ネットワークを介してサーバ１３にアクセスすると（同図（１））、サーバ１３はゲーム装置１１にゲーム装置１１の装置ＩＤと記録媒体１０のＳＮの転送を要求する。装置ＩＤとは各ゲーム装置に対して重複しないように割り与えられた識別情報であり、サーバ１３から発行される。

【００２２】

ゲーム装置１１が初めてサーバ１３にアクセスした場合には、サーバ１３はゲーム装置１１に装置ＩＤを未だ発行していないため、ゲーム装置１１に装置ＩＤを発行する（同図（２））。装置ＩＤとして、ゲーム装置１１がサーバにアクセスした時期を利用することができる。時期には日時である西暦、月、日、時、分、秒が含まれる。例えば、アクセスのあった日時が２０００年１２月１０日２１時５分３７秒であった場合には、装置ＩＤは、２０００．１２．１０．２１．０５．３７となる。ゲーム装置１１はサーバ１３から発行された装置ＩＤをフラッ

シュメモリ等の不揮発性メモリ１２に記憶する。また、この日時を暗号化したデータを装置ＩＤとして不揮発性メモリ１２に記憶してもよい。

【００２３】

データベース１４には装置ＩＤをキーとしてゲーム装置に使用された記録媒体のＳＮが関連付けられてレコード単位で管理されている。サーバ１３はゲーム装置１１に発行した装置ＩＤ（２０００．１２．１０．２１．０５．３７）とＳＮ（Ａ０１０１）を関連付けたレコードを生成する（同図（３））。

【００２４】

上記の構成により、サーバ１３はゲーム装置１１の装置ＩＤと記録媒体１０のＳＮを関連付けて一元的に管理しているため、第三者が他のゲーム装置で使用された記録媒体を自己のゲーム装置に挿入して使用しようとすると、該記録媒体のＳＮとゲーム装置の装置ＩＤが一致しないため、サーバ１３は該第三者の記録媒体の使用に制限をかけることができる。

【００２５】

また、２人以上のプレイヤが秒単位まで含めて同時にサーバにアクセスすることが殆ど皆無であることを考慮すると、装置ＩＤとしてゲーム装置１１がサーバ１３にアクセスした日時を秒単位まで利用することで、実質的に各ゲーム装置に固有の装置ＩＤを割り当てることができる。勿論、装置ＩＤとして、ゲーム装置がサーバにアクセスした日時のみならず予め重複しないように用意したＩＤを利用することもできる。

【００２６】

尚、上記の説明では記録媒体としてＣＤ－ＲＯＭを例示したが、これに限らず、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＤＶＤ－Ｒ、ＰＤディスク、ＭＤディスク、ＭＯディスク等の各種光ディスク、フレキシブルディスク（ＦＤ）、ゲームプログラムを記憶した脱着式カートリッジ、メモリカード等にも適用できる。

【００２７】

発明の実施の形態２．

図３はゲーム装置と操作用コントローラの説明図である。操作用コントローラ２０にはセーブデータを待避保存するためのバックアップメモリ２２を脱着自在

に構成され、さらにアナログキーや各種スイッチを配置した操作部２１が設けられている。バックアップメモリ２２は不揮発性メモリを備えている。操作用コントローラ２０は接続コード２８、及びコネクタ２９を介してゲーム装置２３に接続している。尚、バックアップメモリ２２はゲーム装置２３に直接脱着自在に取り付けるように構成してもよい。

【００２８】

図２はゲーム装置と操作用コントローラの機能ブロック図である。ゲーム装置２３はゲーム処理部２４、暗号処理部２５、ＣＤ－ＲＯＭドライブ２６、装置ＩＤメモリ２７を備えて構成されている。これらの各モジュールはＣＰＵ、ＲＯＭ、ＲＡＭ等のハードウエアによって実現される。ゲーム処理部２４にはＣＤ－ＲＯＭドライブ２６を介してＣＤ－ＲＯＭから供給されるゲームプログラムを読み取り、操作部２１から出力されるアナログキーや各種スイッチの制御信号を基にゲームを展開し、バックアップメモリ２２に待避保存するためのセーブデータを生成する。

【００２９】

プレイヤがセーブデータをバックアップメモリ２２に待避保存するようにゲーム装置２３に指示を与えるか、若しくはゲームプログラムがプログラム処理の過程でセーブデータを待避保存するようにゲーム装置２３に指示を与えると、暗号処理部２５は装置ＩＤメモリ２７に記憶されているゲーム装置２３の固有情報（例えば、製造番号）をキーとしてセーブデータに暗号処理を施し、バックアップメモリ２２に待避保存する。暗号処理は公知の暗号処理を利用することができる。一方、バックアップメモリ２２に記憶されているセーブデータをゲーム装置２３が読み取る場合には、セーブデータは暗号処理部２５にて装置ＩＤをキーとして復号処理され、ゲーム処理部２４に出力される。

【００３０】

上記の構成により、バックアップメモリ２２にセーブされるデータはゲーム装置２３の固有情報をキーとして暗号化処理されるため、他のゲーム装置で利用することができない。従って、他人のバックアップメモリを利用して自己のゲーム装置でゲームプレイする等のバックアップメモリの不正使用を有効に防止するこ

とができる。

【００３１】

発明の実施の形態３．

図４は複数のゲーム装置が通信ットワークに接続してゲームプレイを行うときの説明図である。同図において、符号３２、３４は家庭用ゲーム装置であり、３５は通信ゲームの制御を行うサーバである。符号３６は公衆回線等の通信ネットワークである。ゲーム装置３２にはセーブデータを待避保存するためのバックアップメモリ３１０を備えた操作用コントローラ３１が接続されている。同様に、ゲーム装置３４にもバックアップメモリ３３０を備えた操作用コントローラ３３が接続されている。通信ネットワーク３６における通信プロトコルはオープンネットワークに適したＴＣＰ／ＩＰを用いる。

【００３２】

ゲーム装置３２はゲームの進行に伴い、プレイヤが獲得したアイテムや、得点、ゲーム進行状況等を適宜、ＲＡＭ３２０に書き込む。ＲＡＭ３２０に書き込まれたデータはセーブデータとしてバックアップメモリ３１０に転送可能である。また、プレイヤが獲得したアイテム等は通信ネットワーク３６を介してゲーム装置３４のＲＡＭ３４０に転送することができる。

【００３３】

図５はバックアップメモリに待避保存されたセーブデータを利用して通信ゲームを行うときのバックメモリの状態を示す説明図である。バックアップメモリ３１０にはアイテム等のセーブデータが待避保存されている。ゲーム装置２３がネットワークに接続すると、バックアップメモリ３１０内のセーブデータはゲーム装置２３のＲＡＭ３２０に転送（移動）され、バックアップメモリ３１０内のセーブデータは消去される。このため、ゲーム装置２３が通信ネットワーク３６に接続している間はバックアップメモリ３１０内のセーブデータは空の状態になっている。ゲーム終了時、ＲＡＭ３２０内のセーブデータをバックアップメモリ３１０に待避保存する際には、ＲＡＭ３２０からバックアップメモリ３１０へセーブデータが転送される。

【００３４】

従来ではバックアップメモリ３１０のセーブデータをＲＡＭ３２０に転送する場合には、セーブデータをコピーして転送していたため、ＲＡＭ３２０にセーブデータを転送した後においてもバックアップメモリ３１０内にもセーブデータが待避保存されたままの状態であった。このため、プレイヤがセーブデータの中のパラメータの一部又は全てを他のプレイヤに提供した場合であっても、その後にバックアップメモリ３１０を操作用コントローラ３１から強制的に抜き取ることにより、他人に提供したセーブデータを自己のバックアップメモリ３１０に保存することができる。

【００３５】

しかし、本実施形態によれば、バックアップメモリ３１０内のセーブデータはＲＡＭ３２０にコピーされるのではなく、ＲＡＭ３２０に移動されるため、上記のようなバックアップメモリの不正使用を有効に防止することができる。

【００３６】

発明の実施の形態４．

図６は通信ゲームの制御を行うサーバとゲーム装置の説明図である。同図において、符号４１は家庭用ゲーム装置であり、サーバ４４にアクセスすることで通信ゲームを行うことができる。ゲーム装置４１は操作用コントローラ４２から供給されるプレイヤの操作信号を基にゲームを展開する。操作用コントローラ４２にはセーブデータを待避保存するためのバックアップメモリ４３を備えて構成されている。バックアップメモリ４３は不揮発性メモリで構成されている。

【００３７】

サーバ４４はデータベース４５を備えており、ゲーム装置４１のネットワークへのアクセス回数とアクセス日時（以下、アクセス情報という。）を装置ＩＤをキーとしてレコード単位で記録している。装置ＩＤとはゲーム装置４１に固有の識別情報であり、例えば製造番号や、ゲーム装置４１が初めてネットワークに接続した日時（秒単位まで含む）等である。同図の例ではゲーム装置４１の装置ＩＤはＢ１０１１、アクセス回数は７２回、アクセス日時は２０００年１０月２日１９時１４分３２秒、２０００年１０月４日２１時２５分１１秒、２０００年１０月９日１１時７分５２秒、…、となっている。ゲーム装置４１のアクセス情報

はデータベース４５に登録されとともに、バックアップメモリ４３にも同様の内容が書き込まれる。

【００３８】

同図において、ゲーム装置４１が通信ネットワークを介してサーバ４４にアクセスすると（同図（１））、サーバ４４はゲーム装置４１から装置ＩＤとバックアップメモリ４３内のアクセス情報を取得する。次いで、データベース４５を参照し（同図（２））、装置ＩＤとアクセス情報が整合するか否かをチェックする。複数のゲーム装置が秒単位まで含めて同一の日時にアクセスすることはほぼない事を考慮すると、アクセス情報はバックアップメモリ４３に固有のものと考えられる。このため、ゲーム装置のアクセス情報はバックアップメモリ４３を他のバックアップメモリと識別するための識別情報として機能する。

【００３９】

装置ＩＤとアクセス情報が一致する場合には、サーバ４４はアクセス回数を１だけインクリメントし、アクセス日時を追加記録することでレコード内容を更新する。また同時にバックメモリ４３のアクセス情報も更新する（同図（３））。一方、装置ＩＤとアクセス情報が一致しない場合には、バックアップメモリ４３の不正使用の疑いがあるため、バックアップメモリ４３の使用を制限する。

【００４０】

装置ＩＤとアクセス情報が一致しない場合として、①セーブデータを他人のバックアップメモリにセーブして使用しようとした場合、②セーブデータの不正コピーの疑いがある場合である。①の場合は、装置ＩＤとアクセス回数、及びアクセス日時が全く一致しないため、ゲーム装置４１に使用されていない他のセーブデータを使用しようとしたことがわかる。②の場合は、ゲーム装置４１に使用されたセーブデータであるため、アクセス日時が一部一致するが、アクセス回数が異なるため不正コピーの疑いがある場合である。

【００４１】

②の場合について、図７を参照して詳細に説明する。同図に示すように、バックアップメモリ４３に記録されたセーブデータをバックアップメモリ４６に不正コピーしたとする（同図（１））。バックアップメモリ４３に記録されているア

クセス回数は７２回とすると、バックアップメモリ４６に記録されているアクセス回数も７２回になる。ここで、プレイヤがバックアップメモリ４３を使用すると、バックアップメモリ４３に記録されているアクセス回数は７３回に更新される（同図（２））。また、データベース４５内のレコードも７３回に更新される（同図（３））。ここで、プレイヤがコントローラ４２からバックアップメモリ４３を抜き取り、バックアップメモリ４６を新たに装着してサーバ４４にアクセスすると、バックアップメモリ４６のアクセス回数とデータベース４５に記録されているアクセス回数が異なるため、不正コピーの疑いがあるとわかる（同図（４））。また、セーブデータを予め別の記録媒体にコピーしておいて、その後ゲームを行い、セーブデータを更新し、再度更新前のセーブデータに戻してゲームを行うような、同じバックアップメモリを使用する場合も同様である。

【００４２】

以上、説明したように本実施形態によれば、サーバ４４はゲーム装置４１の装置ＩＤとアクセス情報を一元的に管理しているため、装置ＩＤとアクセス情報を照合することで、バックアップメモリ４３の不正使用、及び不正コピーを有効に防止することができる。

【００４３】

発明の実施の形態５.

図８は複数のゲーム装置を通信ネットワークに接続して通信ゲームを行う場合の説明図である。同図において、符号５１～５３は通信ネットワーク５４に接続するゲーム装置であり、符号５５は通信ゲームの制御を行うサーバである。本実施形態においては、図９に示すように、通信ゲームのレベルに応じてゲーム参加可能なレベルを設定している。例えば、ノーマルレベルでは全員の参加が可能であるが、ハードレベルではレベル２０以上、ベリーハードレベルではレベル４０以上がゲーム参加条件となる。ここでいうレベルとは、ゲームの進行に伴って、プレーヤキャラクタに与えられるパラメータであり、主に、ゲーム中に倒した敵キャラクタの種類や数に対応して与えられる。

【００４４】

図８にはハードレベルの通信ゲームを行う場合の各プレイヤのレベルが記述さ

れており、ゲーム装置５１のプレイヤのレベルは２５、ゲーム装置５２のプレイヤのレベルは３０、ゲーム装置５３のプレイヤのレベルは４５であるから、これら三人のプレイヤでハードレベルの通信ゲームを行うことができる。

【００４５】

従来ではこのような通信ゲームを複数人で行う場合、プレイヤのレベルを問わずに参加可能であったため、例えば、通信ゲームに習熟したベ上級レベルのプレイヤと通信ゲームを始めたばかりの初心者が一緒にゲームプレイすることができ、初心者は上級者レベルのプレイヤの後をついて行くことで、ゲームのエンディングまで辿り着くことが可能となる。このようなレベルの高低を問わずに通信ゲームの自由参加を認めるとゲームの面白さを半減することになりかねない。しかし、本実施形態によれば、通信ゲームのレベルに応じて参加可能なプレイヤのレベルが設定されているため、上記の不都合を解消することができる。

【００４６】

発明の実施の形態６.

図１０はゲーム展開のシナリオを記述した説明図である。同図に示すように、ゲームはステージ１～ステージ３までの各ステージから構成される。ステージは森林地帯、地下洞窟、採掘場、古代宇宙船等の場面からなる。各ステージにはゲームの進行に合わせてシーン１、シーン２が設定されており、場面展開に変化を与えている。各ステージにはラスト場面があり、ここに登場する敵キャラクタを倒すことで次ステージに移行することができる。

【００４７】

プレイヤが通信ネットワークに接続せずにオフラインでゲームプレイする場合には、次回のゲームプレイに備えてゲームの進行状況をフラグデータとしてセーブ（保存）ておくのが一般的である。しかし、通信ネットワークに接続してオンラインでゲームプレイする場合には、複数のプレイヤキャラクタがゲームを展開するため、例えば、初心者は何もしなくても上級レベルのプレイヤの後をつけていくだけでゲームを進行することができる。

【００４８】

このため、本実施形態では図１１に示すように、オンラインでゲームを行う場

合には（ステップＳ１；ＹＥＳ）、ゲーム進行のフラグデータをセーブせず（ステップＳ２）、オンラインでゲームを行わない場合には（ステップＳ１；ＮＯ）、ゲーム進行のフラグデータをセーブする（ステップＳ３）。かかる構成により、上記の不都合を解消することができる。また、ゲーム装置がゲーム進行のフラグデータを保存する場合であっても、通信ネットワークに接続しないでゲームを行うときには該フラグデータを参照してゲームの途中からプレイすることを禁じるように構成してもよい。

【００４９】

尚、通信ゲームの場合にゲーム進行のフラグデータのセーブを制御する手段として、ゲーム装置側にセーブ制御手段を設けてもよく、ゲームサーバの制御によりゲーム進行のフラグデータのセーブを制御するように構成してもよい。

【００５０】

発明の実施の形態７.

図１２にゲームのエンディング画面の画面遷移を示す。同図において、（Ａ１）～（Ａ３）はプレイヤが通信ネットワークに接続せずにオフラインでゲームプレイをし、ゲームを終了したときのエンディング画面の画面遷移図である。プレイヤキャラクタ６１が敵キャラクタ６２を倒し、ゲームが終了すると（同図（Ａ１））、エンディングスタッフロールが数分間流れ（同図（Ａ２））、終了画面が表示される（同図（Ａ３））。

【００５１】

一方、（Ｂ１）～（Ｂ２）は複数人が通信ネットワークに接続してオンラインでゲームプレイをし、ゲームを終了したときのエンディング画面の画面遷移図である。プレイヤキャラクタ７１～７４が敵キャラクタ７５を倒してゲームが終了すると（同図（Ｂ１））、速やかに終了画面が表示され（同図（Ｂ２））、元のゲーム画面に戻る（同図（Ｂ１））。

【００５２】

このように、プレイヤがオンラインで通信ゲームを行う場合には、回線に接続している限り、電話回線の接続料として電話料金が課金される他、サーバへのインターネット接続料金が課金されるため、ゲームのエンディング画面を短時間で

終了することで、プレイヤの経済的負担を軽減することができる。

【００５３】

尚、通信ゲームの場合にゲームのエンディング画面の表示時間を短く制御する手段として、ゲーム装置側に該制御手段を設けてもよく、ゲームサーバの制御によりエンディング画面の表示時間を短く制御するように構成してもよい。

【００５４】

【発明の効果】

本発明のセキュリティシステム、記録媒体管理方法及び該方法をコンピュータシステムに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体によれば、通信ネットワークを介してサーバからデータ処理装置に識別情報が発行されるため、データ処理装置に予め識別情報が与えられていない場合でも、どの記録媒体がどのデータ処理装置に使用されたを管理することができる。

【００５５】

本発明のデータ処理装置、データ処理方法及び該方法をコンピュータシステムに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体によれば、バックアップメモリのセーブデータをデータ処理装置に固有の識別情報をキーにして暗号化処理及び復号化処理をすることができるため、セーブデータのセキュリティ対策に効果的である。

【００５６】

本発明のデータ処理装置及びセーブデータの管理方法によれば、データ処理装置にてデータ処理されるセーブデータをデータ処理装置に転送した後で、バックアップメモリ内の不揮発性メモリに記憶されたセーブデータを消去するため、セーブデータの不正使用を効果的に防止することができる。

【００５７】

本発明のセキュリティシステム、セーブデータの管理方法及び該方法をコンピュータシステムに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体によれば、バックアップメモリを備えたデータ処理装置が通信ネットワークに接続した回数をサーバが管理しているため、バックアップメモリ内のセーブデータの不正使用を効果的に防止することができる。

【００５８】

本発明のゲームサーバによれば、ゲームの難易度に対応して通信ゲームに参加可能なレベルを予め設定し、ゲームの難易度に対応した要求レベルを満たすプレイヤに対して通信ゲームの参加を許可するため、通信ゲームをより面白くすることができる。

【００５９】

本発明のゲーム処理方法及び該方法をゲーム装置に実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体によれば、通信ネットワークに接続して通信ゲームを行うときにはゲームの進行状況をセーブデータとして保存しないため、通信ゲームをより面白くすることができる。

【００６０】

本発明のゲーム処理方法及び該方法をゲーム装置に実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体によれば、通信ネットワークに接続して通信ゲームを行うときにはゲームのエンディング画面の表示時間を短くするため、通信ネットワークの接続料の負担を軽減することができる。

【図面の簡単な説明】

【図１】

記録媒体のセキュリティシステムの説明図である。

【図２】

ゲーム装置とコントローラの説明図である。

【図３】

ゲーム装置とコントローラの外観説明図である。

【図４】

ゲーム装置と通信ネットワークの接続構成を示す説明図である。

【図５】

セーブデータの移動を示す説明図である。

【図６】

バックアップメモリのセキュリティシステムの説明図である。

【図７】

バックアップメモリの不正コピー対策の説明図である。

【図８】

通信ゲームの説明図である。

【図９】

通信ゲーム参加可能レベルの説明図である。

【図１０】

ゲーム展開のシナリオの説明図である。

【図１１】

ゲーム進行のフラグデータのセーブに関するフローチャートである。

【図１２】

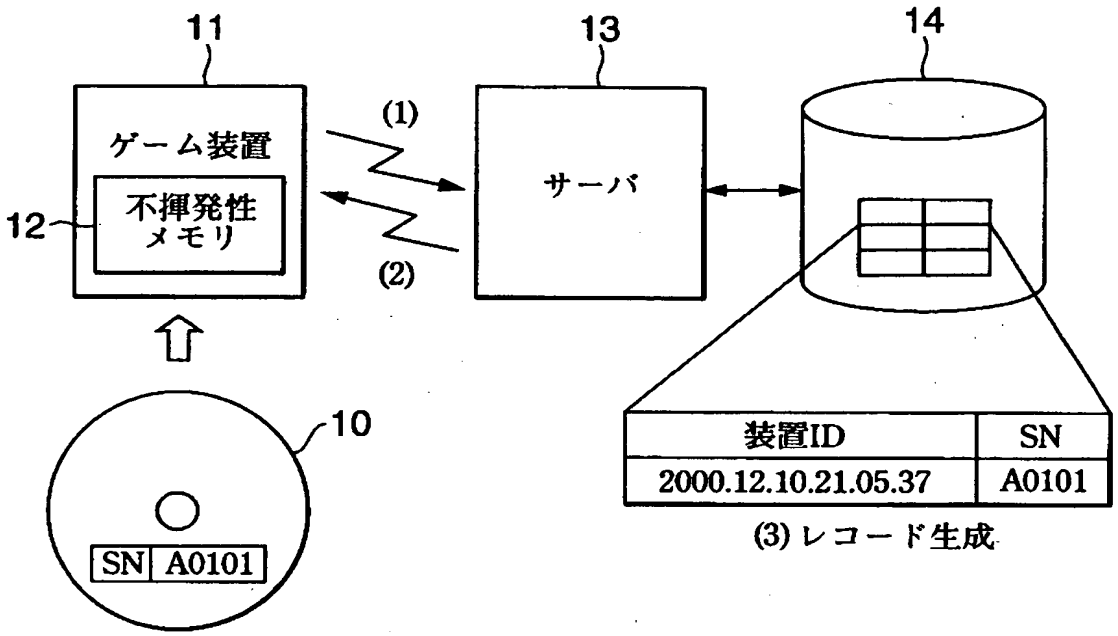
ゲームのエンディング画面の説明図である。

【符号の説明】

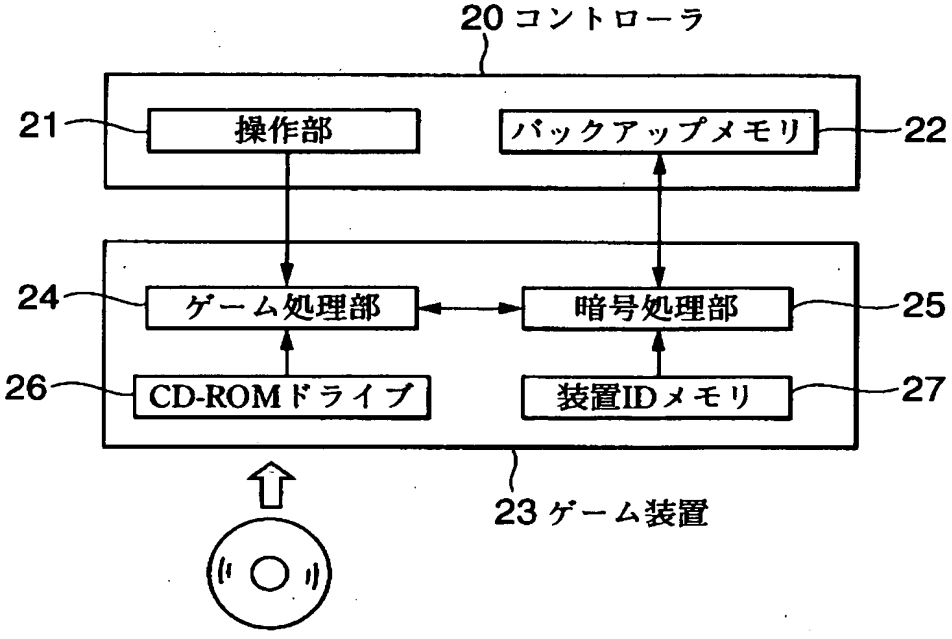
１０…ＣＤ－ＲＯＭ、１１…ゲーム装置、１２…不揮発性メモリ、１３…サーバ、１４…データベース、２０…コントローラ、２１…操作部、２２…バックアップメモリ、２３…ゲーム装置、２４…ゲーム処理部、２５…暗号処理部、２６…ＣＤ－ＲＯＭドライブ、２７…装置ＩＤメモリ、２８…接続コード、２９…コネクタ、３１…コントローラ、３２…ゲーム装置、３３…コントローラ、３４…ゲーム装置、３５…サーバ、３６…通信ネットワーク、３１０…バックアップメモリ、３２０…ＲＡＭ、３３０…バックアップメモリ、３４０…ＲＡＭ、４１…ゲーム装置、４２…コントローラ、４３…バックアップメモリ、４４…サーバ、４５…データベース、４６…バックアップメモリ、５１～５３…ゲーム装置、５４…通信ネットワーク、５５…サーバ

【書類名】　　図面

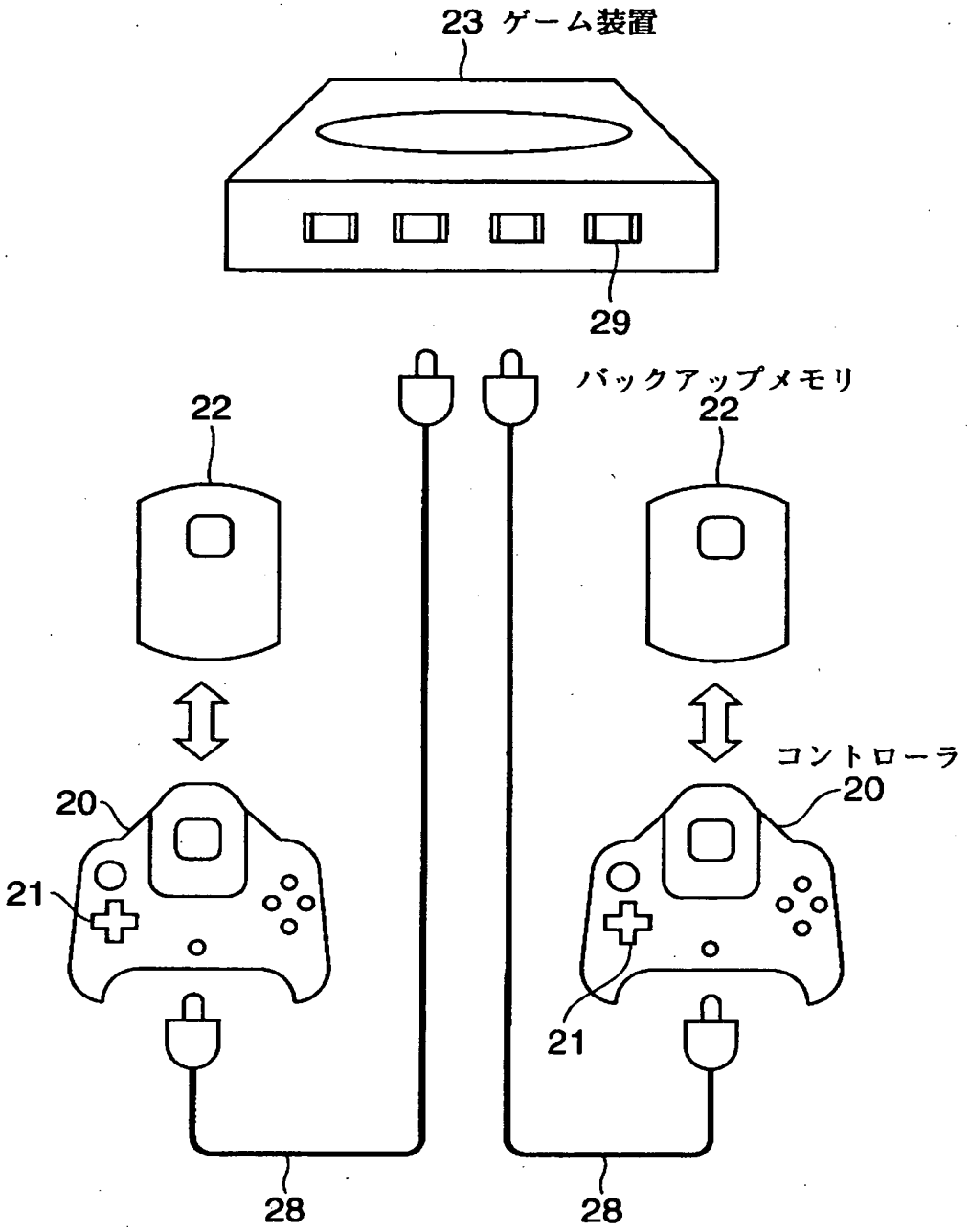
【図１】


11
13
14
ゲーム装置
不揮発性メモリ
12
(1)
(2)
サーバ
10
SN A0101
装置ID
SN
2000.12.10.21.05.37
A0101
(3) レコード生成

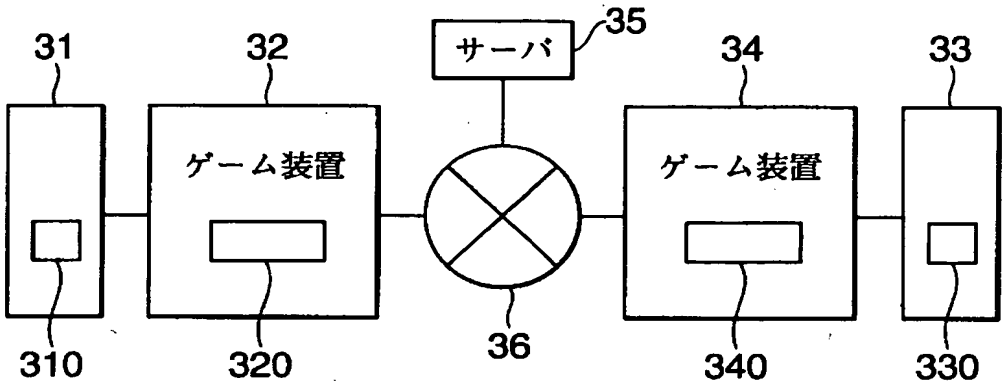
【図２】


20 コントローラ
21
操作部
バックアップメモリ
22
24
ゲーム処理部
暗号処理部
25
26
CD-ROMドライブ
装置IDメモリ
27
23 ゲーム装置

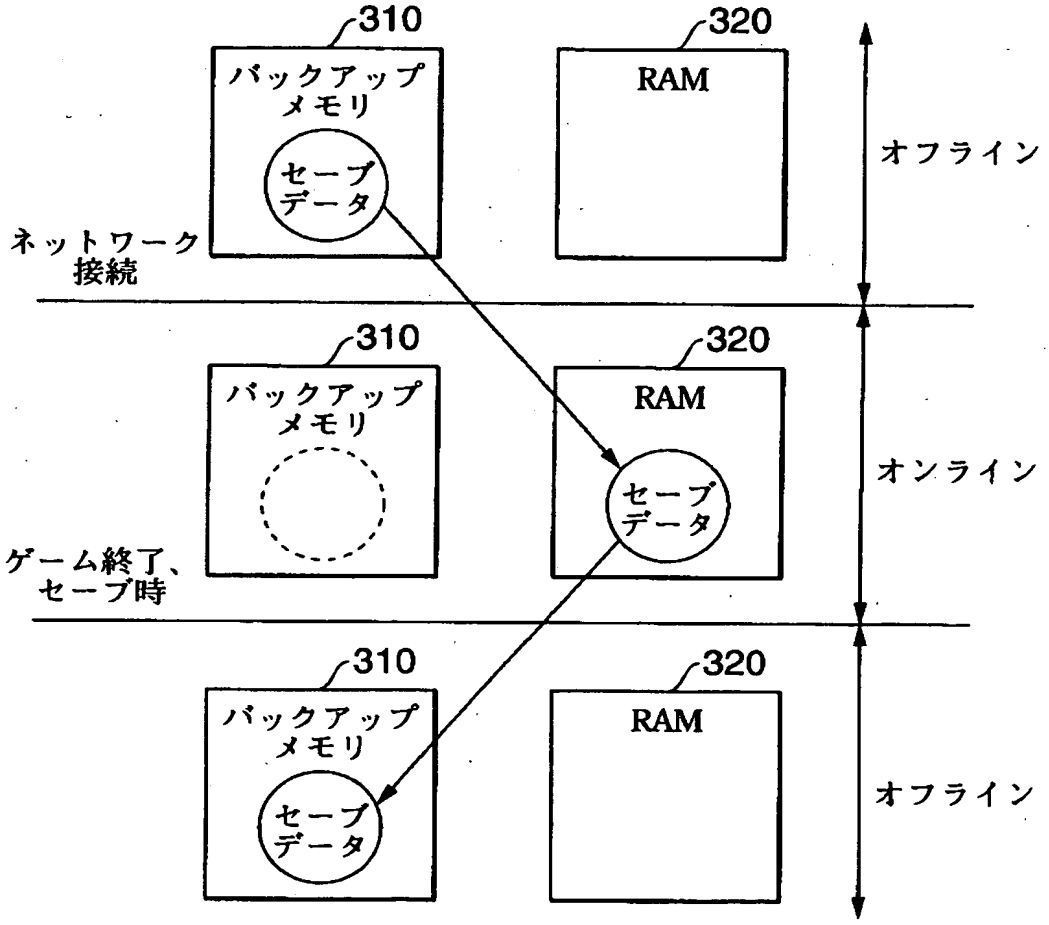
【図３】



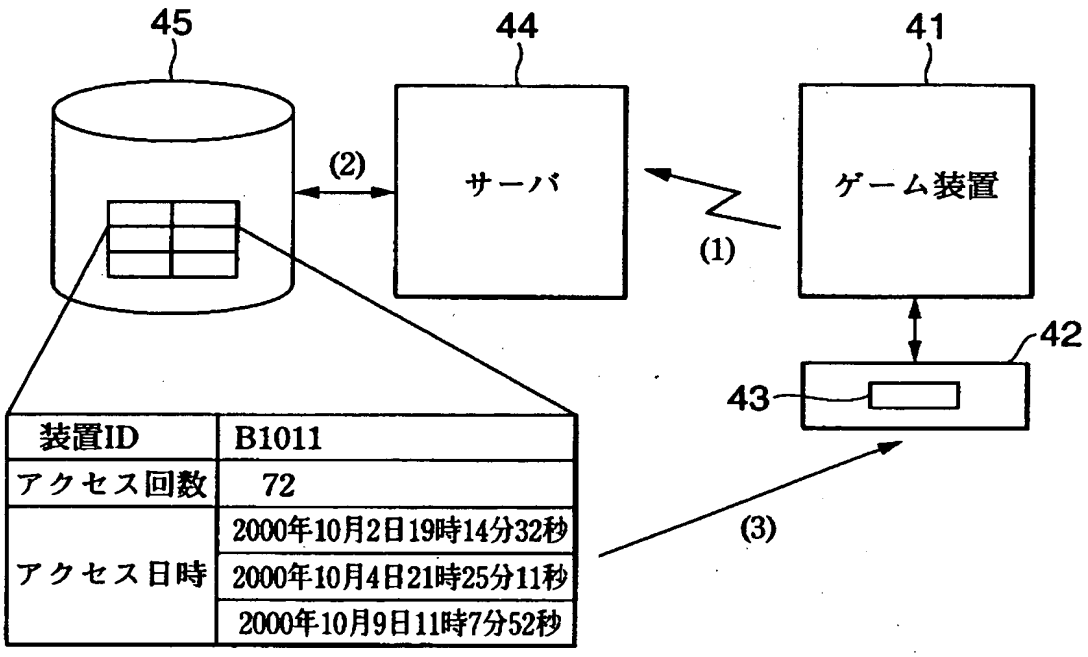
【図４】


31
32
サーバ
35
34
33
ゲーム装置
ゲーム装置
310
320
36
340
330

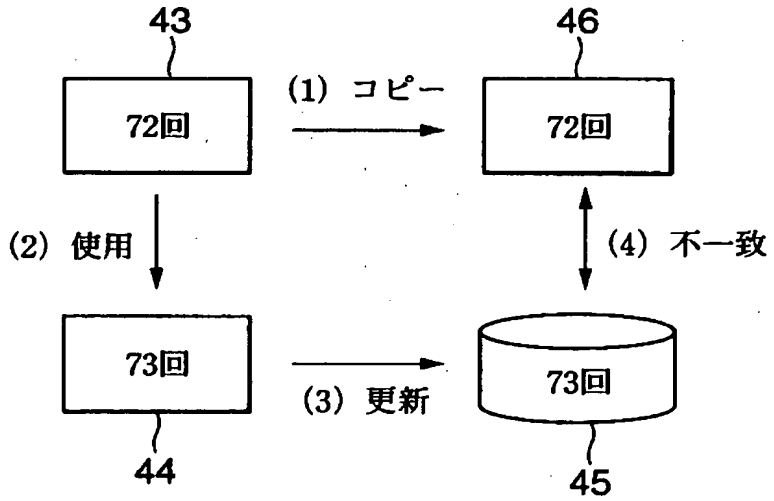
【図５】


310
バックアップ
メモリ
セーブ
データ
320
RAM
オフライン
ネットワーク
接続
310
バックアップ
メモリ
320
RAM
セーブ
データ
オンライン
ゲーム終了、
セーブ時
310
バックアップ
メモリ
セーブ
データ
320
RAM
オフライン

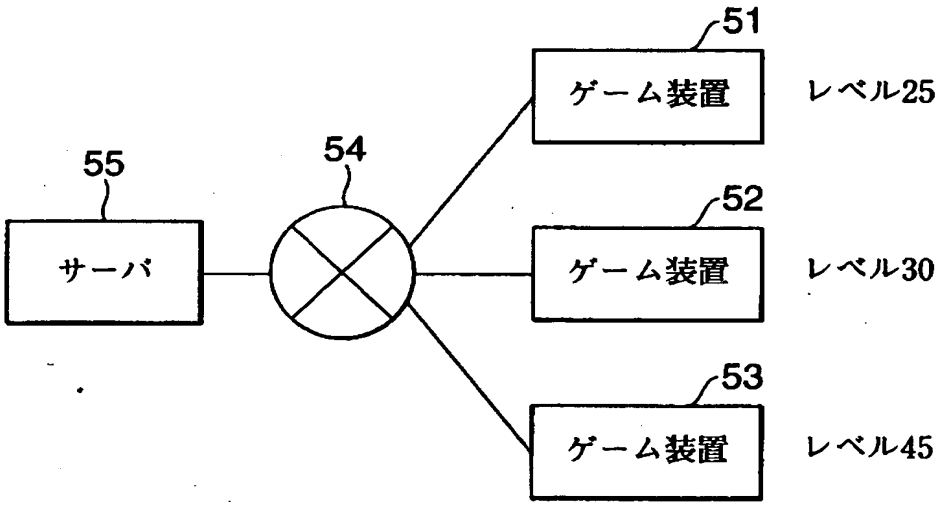
【図６】


45
44
41
(2)
サーバ
ゲーム装置
(1)
42
43
装置ID
B1011
アクセス回数
72
アクセス日時
2000年10月2日19時14分32秒
2000年10月4日21時25分11秒
2000年10月9日11時7分52秒
(3)

【図７】


43
46
72回
(1) コピー
72回
(2) 使用
(4) 不一致
73回
(3) 更新
73回
44
45

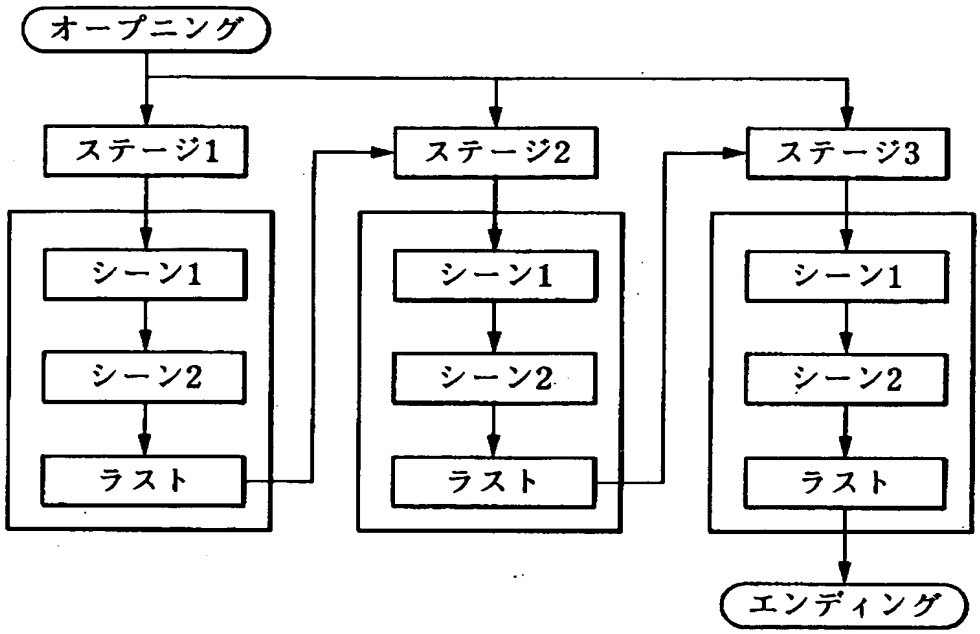
【図８】



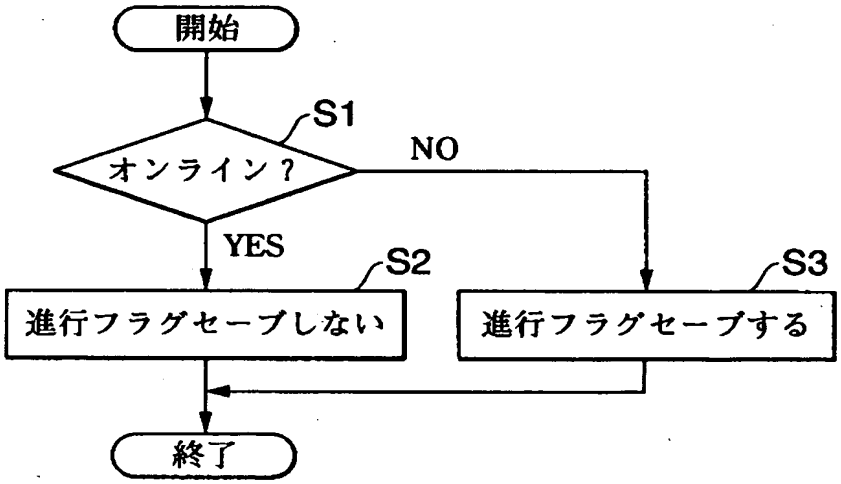
【図９】

モード	必要レベル
ノーマル	全員可
ハード	20以上
ベリーハード	40以上

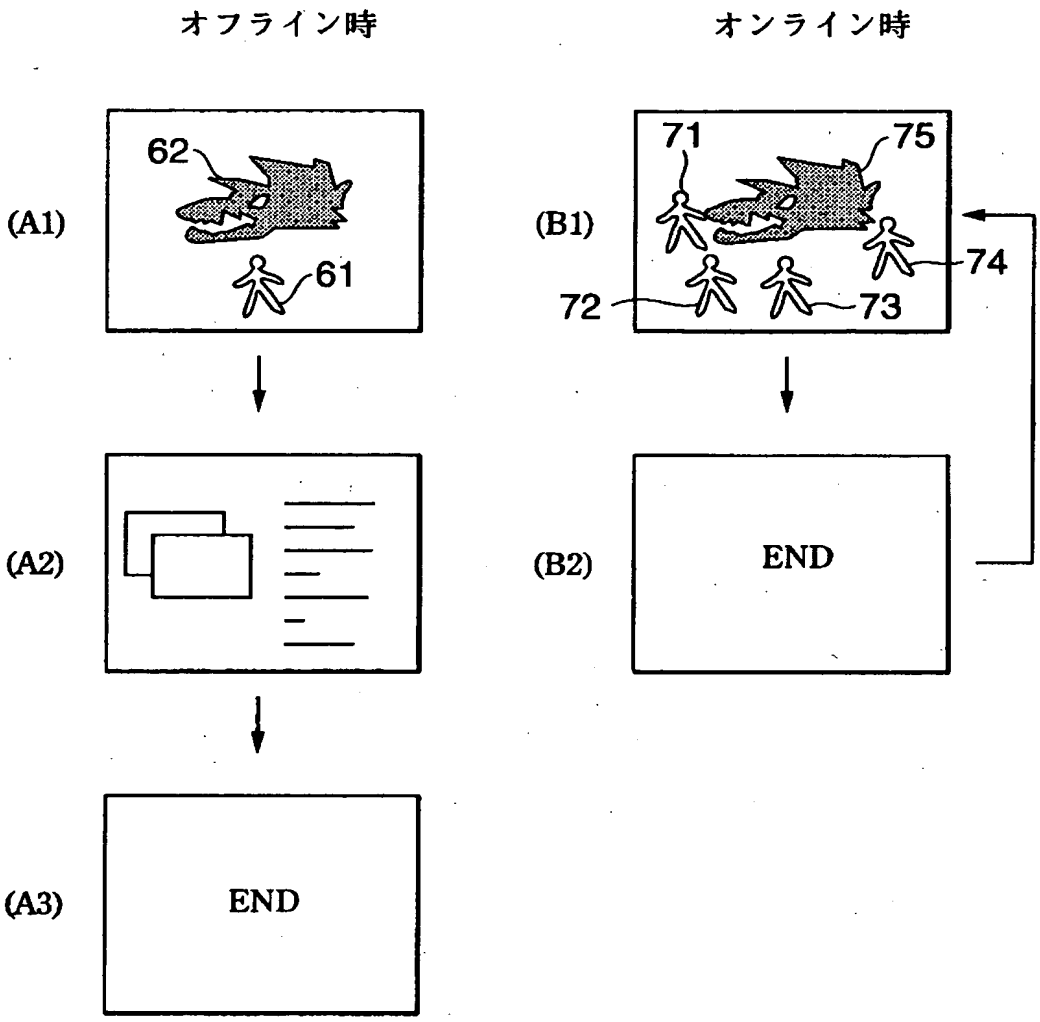
【図１０】


オープニング
ステージ1
ステージ2
ステージ3
シーン1
シーン2
ラスト
シーン1
シーン2
ラスト
シーン1
シーン2
ラスト
エンディング

【図１１】


開始
S1
オンライン？
NO
YES
S2
S3
進行フラグセーブしない
進行フラグセーブする
終了

【図１２】



【書類名】　　要約書

【要約】

【課題】　予め識別情報をもたないゲーム装置に使用されるＣＤ－ＲＯＭがどのゲーム装置に使用されたかを管理するセキュリティシステムを提供する。

【解決手段】　ゲーム装置（１１）は通信ネットワークを介してサーバ（１３）にアクセスすると、サーバ（１３）から発行される装置ＩＤを不揮発性メモリ（１２）に記憶する。この装置ＩＤはゲーム装置（１１）が通信ネットワークを介してサーバ（１３）にアクセスした日時（例えば、２０００年１２月１０日２１時５分３７秒）を基に生成される。サーバ（１３）はゲーム装置（１１）に使用されたＣＤ－ＲＯＭ（１０）のシリアルナンバー（ＳＮ）とゲーム装置（１０）の装置ＩＤを関連付けてデータベース（１４）上に登録する。これにより、どのＣＲ－ＲＯＭ（１０）がどのゲーム装置（１１）で使用されたかを管理することができる。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－３８７８３３
受付番号	５００００１６４６６９８
書類名	特許願
担当官	第三担当上席　００９２
作成日	平成１２年１２月２１日

＜認定情報・付加情報＞

【提出日】　平成12年12月20日

次頁無

出願人履歴情報

識別番号　〔０００１３２４７１〕

１．変更年月日　２０００年１１月　１日
［変更理由］　名称変更
住　所　東京都大田区羽田１丁目２番１２号
氏　名　株式会社セガ